УДК 004.056
DOI 10.33764/2618-981X-2023-6-249-256

Е. П. Усольцева[1], А. В. Шабурова[1]*

Проблема экономической оценки эффективности затрат на защиту персональных данных

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: usoliz@yandex.ru

Аннотация. Защита персональных данных (далее – ПДн) является важнейшей частью защиты информации. С ростом числа кибератак и утечек данных стало крайне важно защищать ПДн от любого несанкционированного доступа или использования. Однако дать оценку экономической эффективности защиты ПДн не так просто. При подготовке к написанию данной статьи не было найдено единой общепринятой методики такой оценки. Для достижения цели исследования в ходе анализа литературы были рассмотрены различные методы экономической оценки эффективности затрат на защиту ПДн: сравнительный анализ, на основе количественной оценки риска информационной безопасности; показатели статистической меры на основе вероятностной модели исходов; метод анализа иерархий; экономико-математическая модель выбора оптимального набора технических средств защиты. В итоге был сделан вывод, что необходимо разработать такой метод экономической оценки эффективности затрат на защиту ПДн, чтобы лучше показать значимость выделяемых средств на защиту ПДн.

Ключевые слова: персональные данные, экономическая эффективность, информационная безопасность

E. P. Usoltseva[1], A. V. Shaburova[1]*

The Problem of Economic Evaluation of the Cost Effectiveness of Personal Data Protection

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: usoliz@yandex.ru

Abstract. Personal data protection (hereinafter referred to as PD) is an essential part of information security. With the increasing number of cyberattacks and data leaks, it has become extremely important to protect PD from any unauthorized access or use. However, it is not so easy to assess the economic effectiveness of PD protection. In preparation for writing this article, no single generally accepted methodology for such an assessment was found. To achieve the purpose of the study, during the analysis of the literature, various methods of economic evaluation of the cost effectiveness of PD protection were considered: comparative analysis, using a quantitative assessment of information security risk (hereinafter referred to as InfoSec); indicators of statistical measures based on a probabilistic outcome model; hierarchy analysis method; economic and mathematical model for choosing the optimal set of technical means of protection. As a result, it was concluded that it is necessary to develop such a method of economic assessment of the cost effectiveness of PD protection in order to show better the significance of the funds allocated for PD protection.

Keywords: personal data, economic efficiency, information security

Введение

В настоящее время ежедневно создается и обновляется огромное количество персональных данных (далее – ПДн). В связи с растущей тенденцией кибератак [1-3] и нарушений конфиденциальности [4] защита ПДн стала достаточно важной темой для субъектов ПДн, правительств и организаций по всему миру.

По данным исследований [5-7], утечки ПДн являются частой проблемой, которая может привести к краже личных средств с банковских счетов, взлому личных электронных почт и т.д. Например, в сфере здравоохранения отмечен рост количества утекших записей (за период январь-сентябрь 2021 г. – январь-сентябрь 2022 г.) (рис. 1).

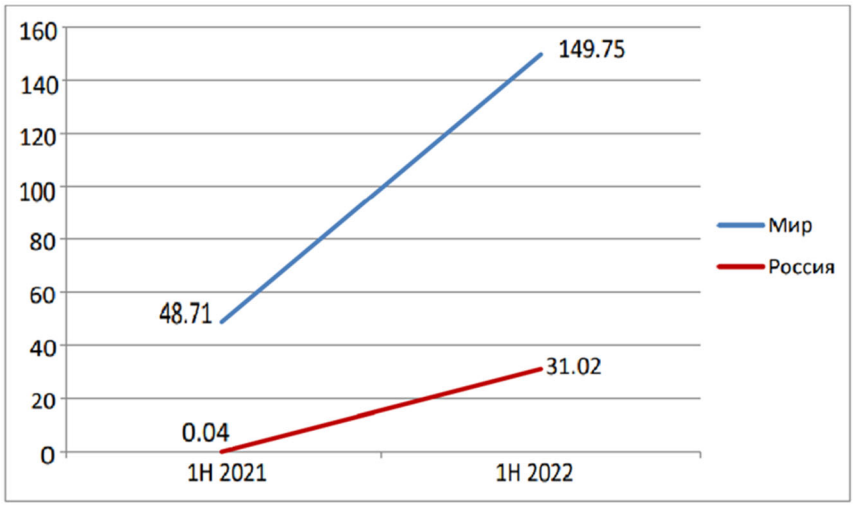

Рис. 1. Количество утекших записей в здравоохранении, млн [7]

Защита ПДн представляется важным фактором в обеспечении доверия граждан и сотрудников по отношению к организации. Как заявил президент компании Salesforce М. Бениофф [8]: «Доверие должно быть наивысшей ценностью в вашей компании, и если это не так, значит, случится что-то плохое». Защита ПДн является необходимым условием для поддержания доверия и сохранения репутации организации.

Примером того, как важно доверие к обеспечению конфиденциальности персональных данных, является ситуация с Агентством национальной безопасности США (АНБ) в 2016 [9], когда стала известно, что АНБ без согласия граждан массово собирали их данные, и эти действия были подвергнуты критике и затем была подана жалоба в суд [10].

В России же, можно привести пример утечек ПДн Яндекс.Еды и Delivery Club [11]. Реакция общественности на штраф в 60 тысяч рублей для такой крупной утечки вызвала резонанс в правительстве [12] и Минцифры совместно с государственными органами и бизнес-сообществом разрабатывают новую систему штрафов за утечку ПДн по словам заместителя директора Департамента обеспечения кибербезопасности Минцифры России Бадягиной А.М. [13].

Так же, оценка эффективности мер обеспечения безопасности ПДн, как правило, производится качественная, а не количественная, но такая оценка не показывает величину возможного материального ущерба, что было бы более наглядно для людей, не имеющих образования по информационной безопасности (далее – ИБ).

Цель статьи: показать, какие методы оценки эффективности затрат на защиту ПДн существуют и показать значимость защиты ПДн.

Методы и материалы

В результате проведенного анализа для описания проблемы авторами было обосновано использование следующих методов:

– метод сравнительного анализа, на основе количественной оценки риска ИБ, который показывает количественную, но не экономическую оценку эффективности;

– метод показателей статистической меры на основе вероятностной модели исходов, который позволяет учитывать разные состояния системы;

– метод анализа иерархий, который учитывает множество критериев и экспертное мнение;

– методический подход к экономической оценке внедрения технических средств защиты информации, который предлагает включение оценки срока окупаемости.

Материалами послужили научные статьи, статистические данные, аналитические исследования организаций, занимающихся ИБ.

Результаты

Согласно пп. 4 п. 2 ст. 19 152-ФЗ часть безопасности ПДн достигается, путем оценки эффективности мер, принятых для обеспечения безопасности ПДн до ввода информационной системы ПДн в эксплуатацию [14]. Не уточняется, что данная оценка должна быть количественная.

Оценка эффективности мер по обеспечению безопасности ПДн, реализуемых в рамках системы защиты ПДн, проводится не реже одного раза в три года в соответствии с приказом ФСТЭК России от 18.02.2013 №21 [15]. Так же не указывается, что нужно проводить количественную оценку.

Оценку эффективности систем защиты производили в научных публикациях [16-19].

В статье [16] предлагается оценивать эффективность мер с помощью сравнительного анализа эффективности системы защиты до и после реализации предложенных мер, с помощью количественной оценки риска ИБ. Для этого, авторы [16] выделяют четыре этапа (рис. 2).

Таким образом, реализация этапов позволит провести оценку эффективности предложенных мер защиты ПДн по критерию сравнительной оценки величины риска ИБ для ИСПДн [16]. Здесь же необходимо отметить, что экономиче-

скую оценку эффективности защиты ПДн авторы не предлагают, но метод важен с точки зрения учета оценки рисков в ИСПДн.

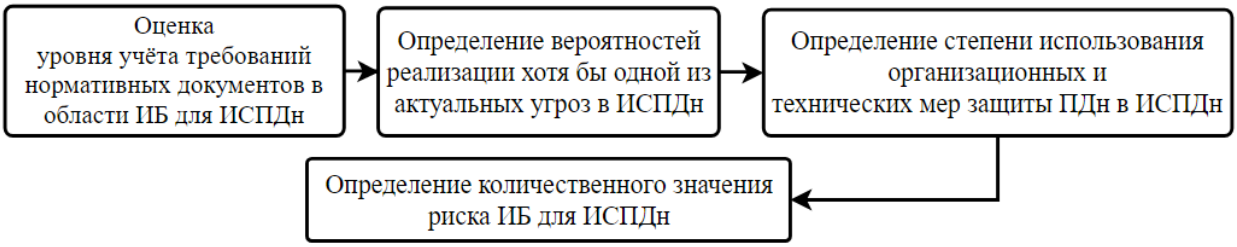

Рис. 2. Этапы оценки риска ИБ для ИСПДн [16]

В публикации [17] было предложено описывать показатели эффективности защиты информации статистической мерой, которая вычисляется с помощью использования вероятностной модели исходов. Так же, было предложено рассматривать разные состояния объектов информационных технологий (далее – ОИТ). Перечень этапов представлен на рис. 3 [17].

Рис. 3. Этапы метода на основе показателей статистической меры, включающей вероятностную модель исходов

С точки зрения обеспечения минимума среднего риска для организаций матрица потерь имеет значение при выборе того, как обеспечить защиту информации. Выбор и построение матрицы потерь – задача, зависящая от заданной цели. В зависимости от выбранных показателя эффективности и пороговой эффектив-

ности элементы матрицы потерь будут иметь различный физический смысл. Так авторы [17] приходят к выводу, что их метод позволяет развить комплексную систему защиты информации.

Авторы следующей статьи [18] предложили метод анализа иерархий. Суть метода состоит в декомпозиции задачи на более простые составные части и дальнейшей обработке последовательных суждений аналитика по парным сравнениям. Для этого, они разделяют метод на этапы (рис. 4).

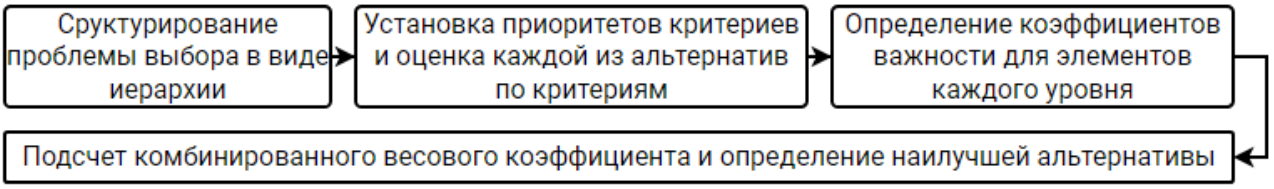

Рис. 4. Алгоритм применения метода анализа иерархий [18]

По мнению авторов [18], использование метода анализа иерархий имеет немало преимуществ. Они заключаются в четкой математической основе метода, легкости вычислительных алгоритмов, возможности изменения системы защиты ПДн, а также учёта множества критериев выбора. Кроме того, метод может быть реализован в программе для работы с электронными таблицами, что также является его достоинством.

В итоге авторы [18] приходят к выводу, что применение метода позволяет наглядно представить общую оценку с учётом выбранных альтернатив. Однако метод основан на экспертном мнении о важности предложенных в методе экономических коэффициентов, что не совсем верно, учитывая, что субъективный фактор может повлиять на точность оценки. Но экспертное мнение может быть важным при обсуждении достоверности полученных результатов.

В публикации [19] была построена экономико-математическая модель выбора оптимального набора технических средств защиты. Для этого метода авторы [19] предлагают следующие этапы (рис. 5).

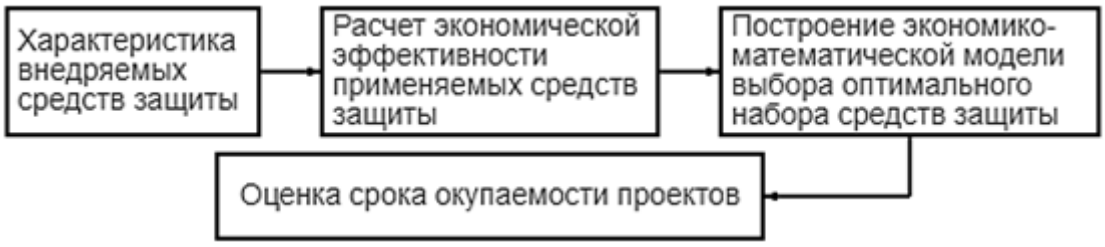

Рис. 5. Этапы методического подхода к экономической оценке внедрения технических средств защиты информации [19]

Расчет экономической эффективности внедряемых мер рассчитали на основе вероятности реализации угроз, путем умножения вероятности реализации

угроз на вероятность уязвимости актива и стоимость ценного актива. Вероятностные значения угроз и ущерба были получены экспертным путем и с использованием статистических данных.

На основе этого в статье [19] сопоставляют стоимость информации и величину возможного ущерба. Далее, была построена экономико-математическая модель выбора оптимального набора технических средств защиты. Затем была произведена оценка срока окупаемости приведенных средств защиты информации.

Метод авторов [19] может применяться для оценки целесообразности инвестиций в проекты с учетом ограничений бюджета, фиксированных затрат и возможной будущей прибыли организаций.

Обсуждение

При написании статьи были проанализированы подходы к оценке экономической эффективности защиты ПДн. Для сравнения были разработаны критерии, которые отображены в табл. 1. Таблица позволяет увидеть, что каждый метод не учитывает все из аспектов.

Таблица 1

Сравнительная таблица методов

Метод	Критерий сравнения					
	Учет требований законодательства	Оценка вероятности рисков ИБ	Стоимость ПДн	Экспертное мнение	Учет состояний ОИТ при воздействии угроз	Оценка срока окупаемости
Сравнительный анализ, с помощью количественной оценки риска ИБ	+	+	-	+	-	-
Показатели статистической меры на основе вероятностной модели исходов	-	+	-	-	+	-
Метод анализа иерархий	-	-	-	+	-	-
Методический подход к экономической оценке внедрения технических средств защиты информации	-	+	+	+	-	+

Учет требований законодательства требуется для учета несения возможной административной и уголовной ответственности за его несоблюдение [12, 14].

Оценка вероятности рисков нужна для оценки возмещения возможного ущерба при реализации таких рисков.

Стоимость ПДн важно учитывать, так как необходимо сопоставить адекватность затраченных средств на защиту ПДн со стоимостью ПДн [20].

Экспертное мнение требуется как при оценке рисков, так и при подведении итогов расчетов.

Учет состояний ОИТ при воздействии угроз так же важен, если, например, в организации или на предприятии имеется несколько баз ПДн и для них используются разные средства защиты.

Оценка срока окупаемости важна, если, к примеру, в данный момент затрачено много средств на защиту ПДн, например, для покупки бессрочной лицензии средства защиты, но далее амортизация такого средства приблизится к нулю.

Таким образом, можно сделать вывод, что нужно разработать такой метод, который учитывает все из выше приведенных аспектов, а именно:

– оценивает риски возникновения угроз на основании законодательства по ПДн;
– учитывает разные состояния ОИТ при воздействии угроз;
– учитывает стоимость (себестоимость) ПДн;
– оценивает сроки окупаемости купленных средств защиты информации.

Заключение

В данной статье авторами были рассмотрены методы оценки экономической эффективности защиты ПДн и сделан сравнительный анализ этих методов. Получен вывод, что необходимо создание метода, который бы включал в себе разные аспекты, указанные в обсуждении.

Важно помнить, что вложения в защиту персональных данных являются инвестицией, которая должна обеспечить надежность используемых средств защиты информации и доверие субъектов ПДн, а также защитить организации от штрафных санкций и прочей ответственности. Однако, даже при наличии надежной системы защиты ПДн необходимо постоянно ее совершенствовать и обновлять, учитывая новые угрозы и требования законодательства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Актуальные киберугрозы: IV квартал 2022 года // Positive Technologies : [сайт]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q4/ (дата обращения: 13.04.2023).

2. Эксперты предсказали рост кибератак на российские компании в 2023 году. Число инцидентов увеличится минимум на 50% // РБК : [сайт]. – URL: https://www.rbc.ru/technology_and_media/13/10/2022/6346cdcc9a7947891c7fd5fc (дата обращения: 13.04.2023).

3. Число кибератак в России и в мире // TAdviser : [сайт]. – URL: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире (дата обращения: 13.04.2023).

4. Как крупные компании расплачиваются за нарушение конфиденциальности данных: 15 кейсов // RB.RU : [сайт]. – URL: https://rb.ru/story/15-privacy-violations/ (дата обращения: 13.04.2023).

5. РКН: 230 млн записей с личными данными россиян утекли в сеть с начала 2022 года // Коммерсантъ RU : [сайт]. – URL: https://www.kommersant.ru/doc/5559664 (дата обращения: 13.04.2023).

6. Group-IB: объём попавших в сеть персональных данных россиян в 2022 году вырос в 40 раз // Хабр : [сайт]. – URL: https://habr.com/ru/news/t/712488/ (дата обращения: 13.04.2023).

7. Утечки конфиденциальной информации в сфере здравоохранения, отчет за 9 месяцев 2022 г. // Экспертно-аналитический центр InfoWatch : [сайт]. – URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-konfidentsialnoy-informatsii-v-sfere-zdravookhraneniya.pdf (дата обращения: 13.04.2023).

8. IN SALESFORCE WE TRUST: HOW CULTURE FEEDS THE BOTTOM LINE / B. Smith / UpperEdge, 2019. URL: https://upperedge.com/salesforce/in-salesforce-we-trust-how-culture-feeds-the-bottom-line/ (дата обращения: 13.04.2023).

9. COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF / ACLU, 2006. URL: https://www.aclu.org/sites/default/files/images/nsaspying/asset_upload_file137_23491.pdf (дата обращения: 13.04.2023).

10. ACLU Sues to Stop Illegal Spying on Americans, Saying President Is Not Above the Law // ACLU : [сайт]. – URL: https://www.aclu.org/press-releases/aclu-sues-stop-illegal-spying-americans-saying-president-not-above-law?redirect=cpredirect/23486 (дата обращения: 13.04.2023).

11. Утечка персональных данных Delivery Club, Яндекс.Еда. Минцифры предлагают штрафовать процентами от оборота за утечку ПДн // MaskSafe : [сайт]. – URL: https://masksafe.ru/news/all/utechka-personalnykh-dannykh-delivery-club-yandeks-eda-mintsifry-predlagayut-shtrafovat-protsentami (дата обращения: 13.04.2023).

12. Предложено наказывать оборотными штрафами компании, допускающие утечку персональных данных // Гарант : [сайт]. – URL: https://www.garant.ru/news/1603061/ (дата обращения: 13.04.2022).

13. Вебинар «Защита персональных данных» [видеозапись] // ВКонтакте : [сайт]. – URL: https://vk.com/rkn?z=video-76229642_456239441%2Fpl_-76229642_-2 (дата обращения: 13.04.2023).

14. Закон Российской Федерации «О персональных данных» от 27.07.2006 № 152 // Собрание законодательства Российской Федерации. – 2006 г. – № 31. – Ст. 3451 с изм. и допол. в ред. от 14.07.2022.

15. Приказ ФСТЭК РФ «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 № 21 // Банк данных «Приказы и распоряжения Министерства юстиции Российской Федерации». – 2013 г. – № 28375. – с изм. и допол. в ред. от 14.05.2020. – URL: https://minjust.consultant.ru/ (дата обращения: 13.04.2023).

16. Курачинова, М.Р. К вопросу об оценке эффективности принимаемых мер защиты персональных данных в информационных системах персональных данных / М.Р. Курачинова, А.А. Шхануков, Д.Е. Юдин // Студенческая наука для развития информационного общества. – 2018. – С.115-118.

17. Кулешов, Ю.Е. Методический подход к оценке эффективности защиты информации / Ю.Е. Кулешов, В.А. Сергиенко, С.И. Паскробка // Проблемы инфокоммуникаций. – 2018. – №1. – С.45-53.

18. Клиндух, О.В. Оценка эффективности защитных мер персональных данных в учебном заведении на основе метода анализа иерархий / О.В. Клиндух, А.А. Рычкова // Новые импульсы развития: вопросы научных исследований. – 2021. – №4. – С. 58-65.

19. Козьминых, С.И. Методический подход к экономической оценке внедрения технических средств защиты информации в кредитно-финансовой организации / С.И. Козьминых // Вопросы кибербезопасности. – 2020. – №3 (37). – С. 87-96.

20. Усольцева, Е.П. Проблема оценки стоимости персональных данных / Е.П. Усольцева, А.В. Шабурова // Интерэкспо Гео-Сибирь. – 2022. – Т. 6. – С. 268-274.